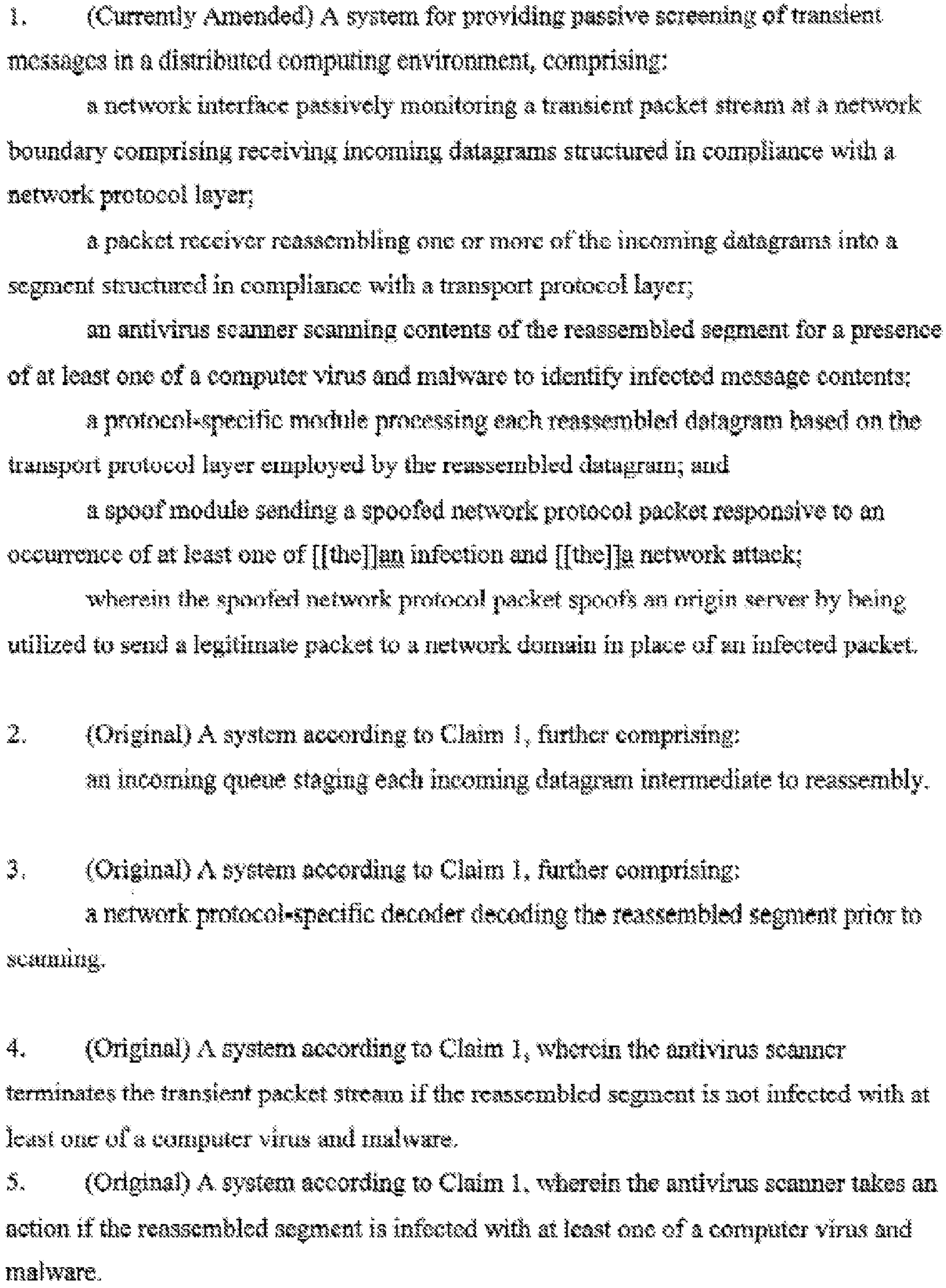
EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Kevin Zilka on 7/23/2008.

The application has been amended as follows:

Please replace the claims with the claim listing which begins on the following page.



1. (Currently Amended) A system for providing passive screening of transient messages in a distributed computing environment, comprising:

a network interface passively monitoring a transient packet stream at a network boundary comprising receiving incoming datagrams structured in compliance with a network protocol layer;

a packet receiver reassembling one or more of the incoming datagrams into a segment structured in compliance with a transport protocol layer;

an antivirus scanner scanning contents of the reassembled segment for a presence of at least one of a computer virus and malware to identify infected message contents;

a protocol-specific module processing each reassembled datagram based on the transport protocol layer employed by the reassembled datagram; and

a spoof module sending a spoofed network protocol packet responsive to an occurrence of at least one of [[the]]an infection and [[the]]a network attack;

wherein the spoofed network protocol packet spoofs an origin server by being utilized to send a legitimate packet to a network domain in place of an infected packet.

2. (Original) A system according to Claim 1, further comprising:

an incoming queue staging each incoming datagram intermediate to reassembly.

3. (Original) A system according to Claim 1, further comprising:

a network protocol-specific decoder decoding the reassembled segment prior to scanning.

4. (Original) A system according to Claim 1, wherein the antivirus scanner terminates the transient packet stream if the reassembled segment is not infected with at least one of a computer virus and malware.

5. (Original) A system according to Claim 1, wherein the antivirus scanner takes an action if the reassembled segment is infected with at least one of a computer virus and malware.

6. (Previously Presented) A system according to Claim 5, wherein the action comprises at least one of logging the infection; generating a warning; spoofing a valid datagram in place of the infected datagram; and acquiescing to the infection.

7. (Original) A system according to Claim 1, further comprising:
a protocol-specific queue staging each reassembled segment with other reassembled segments sharing the same transport protocol layer.

8. (Original) A system according to Claim 7, further comprising:
an information record storing information dependent on the same transport protocol layer with the staged reassembled segment.

9. (Original) A system according to Claim 8, further comprising:
a contents record storing the contents with the staged reassembled segment.

10. (Original) A system according to Claim 8, wherein the information comprises at least one of a source address, source port number, destination address, destination port number, URL, file name, user name, sender identification, recipient identification, and subject.

11-12. (Cancelled)

13. (Original) A system according to Claim 1, further comprising:
an event correlator analyzing the transient packet stream for events indicative of a network service attack.

14. (Original) A system according to Claim 13, further comprising:
a data repository maintaining each event.

15. (Original) A system according to Claim 1, wherein the distributed computing environment is TCP/IP-compliant and each incoming message is SMTP-compliant

16. (Previously Presented) A method for providing passive screening of transient messages in a distributed computing environment, comprising:

passively monitoring a transient packet stream at a network boundary comprising receiving incoming datagrams structured in compliance with a network protocol layer;

reassembling one or more of the incoming datagrams into a segment structured in compliance with a transport protocol layer;

scanning contents of the reassembled segment for a presence of at least one of a computer virus and malware to identify infected message contents;

processing each reassembled datagram based on the transport protocol layer employed by the reassembled datagram; and

sending a spoofed network protocol packet responsive to an occurrence of at least one of an infection and a network attack;

wherein the spoofed network protocol packet spoofs an origin server by being utilized to send a legitimate packet to a network domain in place of an infected packet.

17. (Original) A method according to Claim 16, further comprising:

staging each incoming datagram intermediate to reassembly.

18. (Original) A method according to Claim 16, further comprising:

decoding the reassembled segment prior to scanning.

19. (Original) A method according to Claim 16, further comprising:

terminating the transient packet stream if the reassembled segment is not infected with at least one of a computer virus and malware.

20. (Original) A method according to Claim 16, further comprising:

taking an action if the reassembled segment is infected with at least one of a computer virus and malware.

21. (Previously Presented) A method according to Claim 20, further comprising:

executing the action, comprising at least one of:
logging the infection;
generating a warning;
spoofing a valid datagram in place of the infected datagram; and
acquiescing to the infection.

22. (Original) A method according to Claim 16, further comprising:
staging each reassembled segment with other reassembled segments sharing the same transport protocol layer.

23. (Original) A method according to Claim 22, further comprising:
storing information dependent on the same transport protocol layer with the staged reassembled segment.

24. (Original) A method according to Claim 23, further comprising:
storing the contents with the staged reassembled segment.

25. (Original) A method according to Claim 23, wherein the information comprises at least one of a source address, source port number, destination address, destination port number, URL, file name, user name, sender identification, recipient identification, and subject.

26-27. (Cancelled)

28. (Original) A method according to Claim 16, further comprising:
analyzing the transient packet stream for events indicative of a network service attack.

29. (Original) A method according to Claim 28, further comprising:
maintaining each event in a data repository.

30. (Original) A method according to Claim 16, wherein the distributed computing environment is TCP/IP-compliant and each incoming message is SMTP-compliant.

31. (Previously Presented) A computer-readable storage medium holding code for performing the method according to Claims 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 28, 29, or 30.

32. (Previously Presented) A system for passively detecting computer viruses and malware and denial of service-type network attacks in a distributed computing environment, comprising:

a network interface receiving copies of datagrams transiting a boundary of a network domain into an incoming packet queue, each datagram being copied from a packet stream;

a packet receiver reassembling one or more such datagrams from the incoming packet queue into network protocol packets, each staged in a reassembled packet queue;

an antivirus scanner scanning each network protocol packet from the reassembled packet queue to ascertain an infection of at least one of a computer virus and malware;

an event correlator evaluating events identified from the datagrams in the packet stream to detect a denial of service-type network attack on the network domain; and

a spoof module sending a spoofed network protocol packet responsive to an occurrence of at least one of the infection and the network attack;

wherein a protocol-specific module processes each reassembled datagram based on an upper protocol layer employed by the reassembled datagram;

wherein the spoofed network protocol packet spoofs an origin server by being utilized to send a legitimate packet to the network domain in place of an infected packet.

33. (Original) A system according to Claim 32, further comprising:

a parser parsing each reassembled datagram into network protocol-specific information and packet content.

34. (Original) A system according to Claim 33, wherein the network protocol-specific information comprises a source address, source port number, destination address, destination port number, and URL for HTTP; a file name and user name for FTP; and a sender identification, recipient identification, and subject for SMTP.

35. (Original) A system according to Claim 33, further comprising:

a decoder decoding the packet content prior to performing the operation of scanning.

36. (Original) A system according to Claim 32, further comprising:

a log logging an occurrence of at least one of the infection and the network attack.

37. (Original) A system according to Claim 32, further comprising:

a warning module generating a warning responsive to an occurrence of at least one of the infection and the network attack.

38-39. (Cancelled)

40. (Original) A system according to Claim 32, wherein the distributed computing environment is TCP/IP-compliant, each datagram is IP-compliant, and each network protocol packet is TCP-compliant.

41. (Previously Presented) A method for passively detecting computer viruses and malware and denial of service-type network attacks in a distributed computing environment, comprising:

receiving copies of datagrams transiting a boundary of a network domain into an incoming packet queue, each datagram being copied from a packet stream;

reassembling one or more such datagrams from the incoming packet queue into network protocol packets, each staged in a reassembled packet queue;

scanning each network protocol packet from the reassembled packet queue to ascertain an infection of at least one of a computer virus and malware;

evaluating events identified from the datagrams in the packet stream to detect a denial of service-type network attack on the network domain; and

sending a spoofed network protocol packet responsive to an occurrence of at least one of the infection and the network attack;

wherein a protocol-specific module processes each reassembled datagram based on an upper protocol layer employed by the reassembled datagram;

wherein the spoofed network protocol packet spoofs an origin server by being utilized to send a legitimate packet to the network domain in place of an infected packet.

42. (Original) A method according to Claim 41, further comprising:

parsing each reassembled datagram into network protocol-specific information and packet content.

43. (Original) A method according to Claim 42, wherein the network protocol-specific information comprises a source address, source port number, destination address, destination port number, and URL for HTTP; a file name and user name for FTP; and a sender identification, recipient identification, and subject for SMTP.

44. (Original) A method according to Claim 42, further comprising:

decoding the packet content prior to performing the operation of scanning.

45. (Original) A method according to Claim 41, further comprising:

logging an occurrence of at least one of the infection and the network attack.

46. (Original) A method according to Claim 41, further comprising:

generating a warning responsive to an occurrence of at least one of the infection and the network attack.

47-48. (Cancelled)

49. (Original) A method according to Claim 41, wherein the distributed computing environment is TCP/IP-compliant, each datagram is IP-compliant, and each network protocol packet is TCP-compliant.

50. (Previously Presented) A computer-readable storage medium holding code for performing the method according to Claims 41, 42, 43, 44, 45, 46, or 49.

51. (Previously Presented) A system according to Claim 32, wherein the network protocol packets employ at least one of HTTP, FTP, SMTP, POP3, NNTP, and Gnutella network protocols.

52. (Previously Presented) A system according to Claim 32, wherein only datagrams compliant with IP protocol are reassembled.

53. (Previously Presented) A system according to Claim 32, wherein the antivirus scanner includes a plurality of protocol-specific scanning submodules, each protocol-specific scanning submodule designated for scanning network protocol packets of a particular protocol.

54. (Previously Presented) A system according to Claim 53, wherein the protocol-specific scanning submodules include an HTTP submodule, an FTP submodule, an SMTP submodule, and an NNTP submodule.

55. (Previously Presented) A system according to Claim 1, wherein the incoming datagrams include IP datagrams that are reassembled into TCP segments.

56. (Cancelled)

57. (Previously Presented) A system according to Claim 53, wherein each of the protocol-specific scanning submodules is used for retrieving a re-assembled packet from an associated protocol-specific queue.

58. (Previously Presented) A system according to Claim 57, wherein the packet receiver maintains each protocol-specific queue at a constant size in accordance with the antivirus scanner.

Drawings

The drawings filed on 2/1/2002 are acceptable subject to correction of the informalities indicated below. In order to avoid abandonment of this application, correction is required in reply to the Office action. The correction will not be held in abeyance.

Fig. 8 Step 111 shows "TCP?" and provides two answers to the question, both answers being "No". The answer directed to step 113 should read "Yes".

Reasons for Allowance

The following is an examiner's statement of reasons for allowance:

While the prior art teaches monitoring a packet stream in order to detect virus infected packets or network attacks, the prior art does not teach doing so passively, as claimed, while also spoofing a network protocol packet by sending a legitimate packet to a network domain in place of an infected packet, in the particular combination of limitations as claimed.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Oath/Declaration

This application presents a claim for subject matter not originally claimed or embraced in the statement of the invention. In this case, the new subject matter is subject matter of claims 53-54, and 57-58. A supplemental oath or declaration is required under 37 CFR 1.67. The new oath or declaration must properly identify the application of which it is to form a part, preferably by application number and filing date in the body of the oath or declaration. See MPEP §§ 602.01 and 602.02.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MATTHEW T. HENNING whose telephone number is (571)272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Matthew T Henning/
Patent Examiner, Art Unit 2131

/Ayaz R. Sheikh/

Supervisory Patent Examiner, Art Unit 2131